Galois Theory §53

Def 53.1 A finite extension K of F is a finite normal extension of F if K is a separable splitting field over F.

$$|G(K/F)| \qquad \{K:F\} \qquad [K:F]$$

Def 53.5

Thm 53.6.

(Main Theorem of Galois Theory) Let K be a finite normal extension of a field F, with Galois group $G(K/F)$. For a field E, where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then λ is a one-to-one map of the set of all such intermediate fields E onto the set of all subgroups of $G(K/F)$. The following properties hold for λ:

1. $\lambda(E) = G(K/E)$.
2. $E = K_{G(K/E)} = K_{\lambda(E)}$.
3. For $H \leq G(K/F)$, $\lambda(K_H) = H$.
4. $[K : E] = |\lambda(E)|$ and $[E : F] = (G(K/F) : \lambda(E))$, the number of left cosets of $\lambda(E)$ in $G(K/F)$.
5. E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When $\lambda(E)$ is a normal subgroup of $G(K/F)$, then
$$G(E/F) \simeq G(K/F)/G(K/E).$$
6. The diagram of subgroups of $G(K/F)$ is the inverted diagram of intermediate fields of K over F.

$K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ $\quad F = \mathbb{Q}$

K is splitting field of $\left\{ \begin{matrix} x^2-2, \\ x^2-5 \end{matrix} \right\}$

$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4.$

$\{K : \mathbb{Q}\} = 1 + 1 + 1 + 1 = 4$

- $id : K \to K$
- $\sigma : K \to K$ $\quad \sigma(\sqrt{2}) = -\sqrt{2}$
  σ fixes $\mathbb{Q}$. $\quad \sigma(\sqrt{5}) = \sqrt{5}$
- $\tau : K \to K$ $\quad \tau(\sqrt{5}) = -\sqrt{5}$ fixes $\mathbb{Q}$
  $\tau(\sqrt{2}) = \sqrt{2}.$
- $\gamma : K \to K$ $\quad \gamma(\sqrt{5}) = -\sqrt{5}$ fixes $\mathbb{Q}$
  $\gamma(\sqrt{2}) = -\sqrt{2}$

$G(K/F) = \{id, \sigma, \tau, \gamma\}.$

all elts have order 2 or 1.

$G(K/F) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

(Main Theorem of Galois Theory) Let K be a finite normal extension of a field F, with Galois group $G(K/F)$. For a field E, where $F \leq E \leq K$, let $\lambda(E)$ be the subgroup of $G(K/F)$ leaving E fixed. Then λ is a one-to-one map of the set of all such intermediate fields E onto the set of all subgroups of $G(K/F)$. The following properties hold for λ:

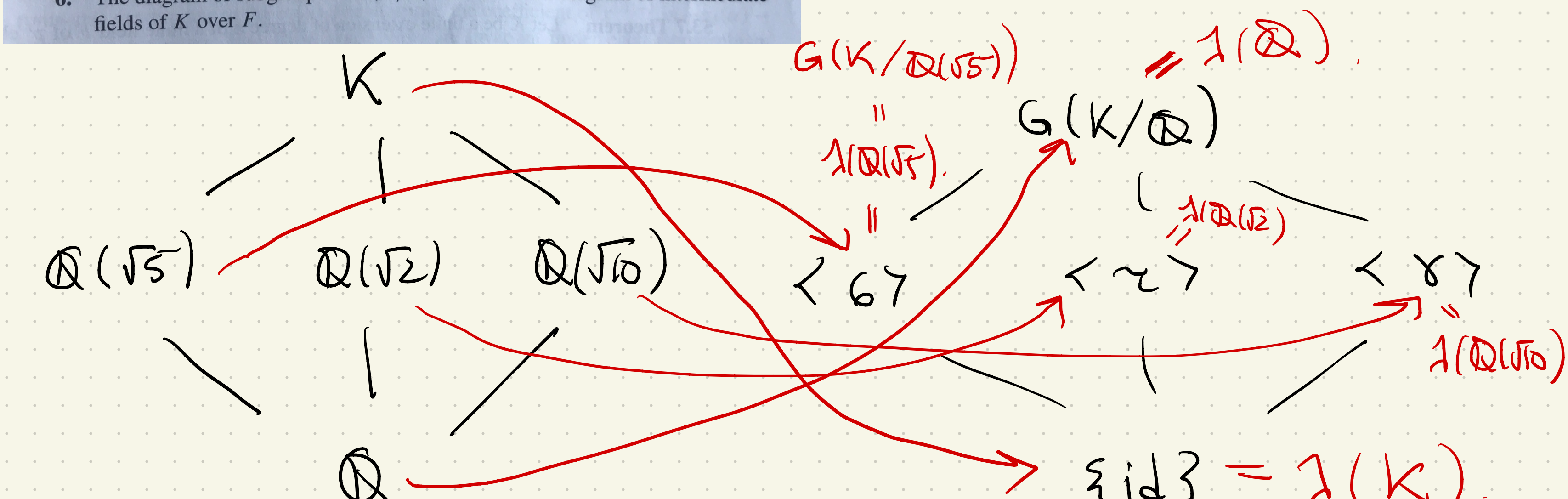
1. $\lambda(E) = G(K/E)$.
2. $E = K_{G(K/E)} = K_{\lambda(E)} = \{\alpha \in K \mid \varphi(\alpha) = \alpha \ \forall\, \varphi \in G(K/E)\}$.
3. For $H \leq G(K/F)$, $\lambda(K_H) = H$. $\Rightarrow$ surjectivity.
4. $[K : E] = |\lambda(E)| = |G(K/E)|$ and $[E : F] = (G(K/F) : \cancel{\lambda(E)})$ $G(K/E)$, the number of left cosets of $\lambda(E)$ in $G(K/F)$.
5. E is a normal extension of F if and only if $\lambda(E)$ is a normal subgroup of $G(K/F)$. When $\lambda(E)$ is a normal subgroup of $G(K/F)$, then
$$G(E/F) \simeq G(K/F)/G(K/E).$$
6. The diagram of subgroups of $G(K/F)$ is the inverted diagram of intermediate fields of K over F.

if $H \leq G(K/\mathbb{Q})$ then

$|H| = 1, 2, 4.$

$K = \mathbb{Q}(\sqrt{2}, \sqrt{5}).$

$\lambda(K) = G(K/K) = \{id\}.$



Intermediate field diagram

subgroup diagram

Example. $F = \mathbb{Q}$ Let K be splitting field of $x^3 - 2$

zeros of $x^3 - 2$ are $\underset{\alpha_1}{\sqrt[3]{2}}$, $\underset{\alpha_2}{e^{2\pi i/3}\sqrt[3]{2}}$, $\underset{\alpha_3}{e^{4\pi i/3}\sqrt[3]{2}}$.

$$K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2}) \quad [K:\mathbb{Q}] = [K:\mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$$

$$= 2 \cdot 3 = 6$$

$$[\mathbb{Q}(\alpha_2):\mathbb{Q}] = 3$$

$\zeta = e^{2\pi i/3}$ is a zero of $x^3 - 1 = (x-1)(x^2+x+1)$ ← irreducible poly ζ over $\mathbb{Q}$ or $\mathbb{Q}(\sqrt[3]{2})$.

aside

$$\mathbb{Q}(\alpha_2) = \{a_0 + a_1\alpha_2 + a_2\alpha_2^2 \mid a_i \in \mathbb{Q}\}$$

$\mathbb{Q}(\alpha_2) \neq K$ since $\nexists$ $a_0, a_1, a_2 \in \mathbb{Q}$ s.t. the above sum $= \sqrt[3]{2}$.

The Galois gp $G(K/\mathbb{Q})$ has size $6 = [K:\mathbb{Q}]$.

An automorphism of $K = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2})$ fixing $\mathbb{Q}$ is determined by where it sends $\{\alpha_1, \alpha_2, \alpha_3\}$

moreover it must send $\alpha_i \longrightarrow \alpha_j$ since field isomorphisms send $\alpha \in K$ to their conjugates.

$\Rightarrow$ any permutation of the set $\{\alpha_1, \alpha_2, \alpha_3\}$ gives an elt of $G(K/\mathbb{Q})$. Hence $G(K/\mathbb{Q}) \cong S_3$

φ " $\longmapsto$ " 6 permutation of indices of $\alpha_1, \alpha_2, \alpha_3$ given by φ.

What are the subgroups of $G(K/\mathbb{Q}) \cong S_3$?

$H \leq S_3$ has order 1, 2, 3, 6 by Lagrange's thm

$|H| = 1 \Rightarrow H = \{id\}$

$|H| = 2 \Rightarrow H = \langle (1,2) \rangle, \langle (2,3) \rangle, \langle (1,3) \rangle$

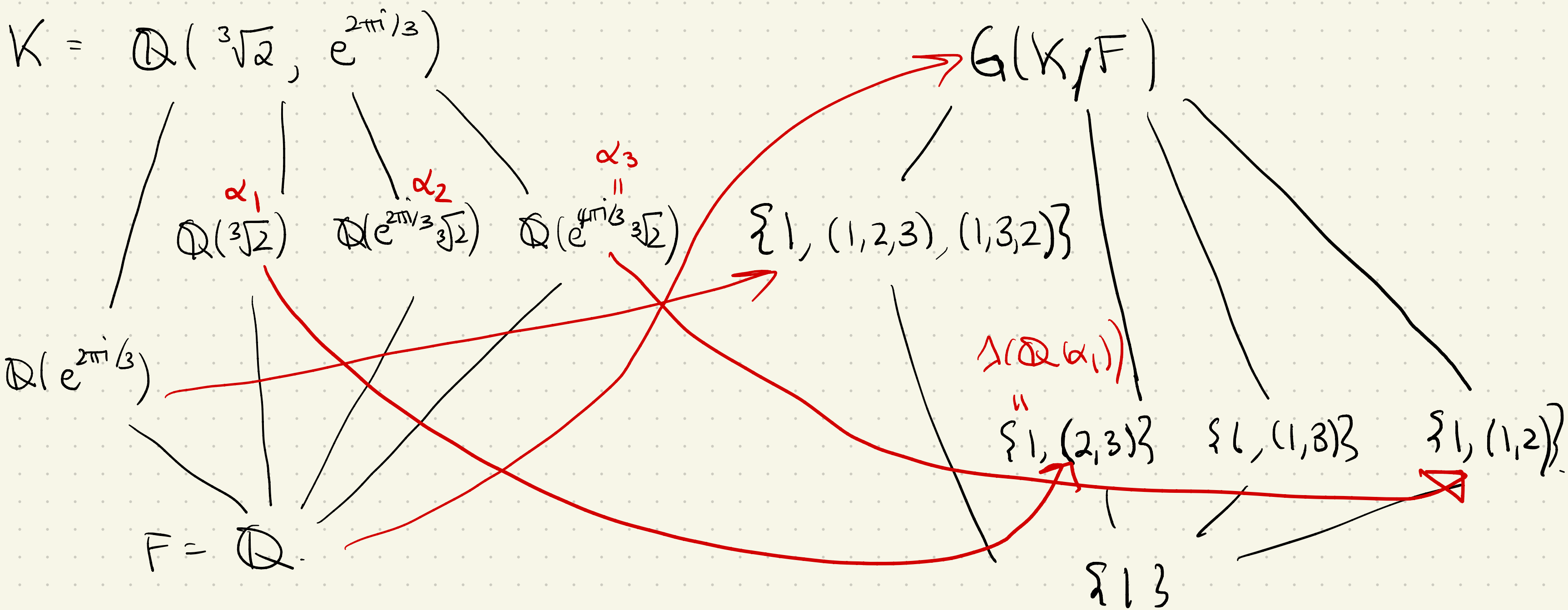
where $\sigma = (1,2)$ means $\varphi_\sigma : K \to K$ $\quad \varphi_\sigma(\alpha_1) = \alpha_2 \quad \varphi_\sigma(\alpha_2) = \alpha_1 \quad \varphi(\alpha_3) = (\alpha_3)$

$|H| = 3 \Rightarrow H = \langle (1,2,3) \rangle = \{id, (1,2,3), (1,3,2)\}$

$\tau = (1,2,3)$ means $\varphi_\tau : K \to K \quad \varphi_\tau(\alpha_1) = \alpha_2 \quad \varphi_\tau(\alpha_2) = \alpha_3 \quad \varphi_\tau(\alpha_3) = \alpha_1$

$$e^{2\pi i/3} = \frac{\sqrt[3]{2}\, e^{2\pi i/3}}{\sqrt[3]{2}} = \frac{\alpha_2}{\alpha_1} \qquad \varphi_\tau\left(\frac{\alpha_2}{\alpha_1}\right) = \frac{\alpha_3}{\alpha_2} = \frac{\sqrt[3]{2}\, e^{4\pi i/3}}{\sqrt[3]{2}\, e^{2\pi i/3}}$$

$|H| = 6 \Rightarrow H = G(K/\mathbb{Q})$



$$[K : \mathbb{Q}(\alpha_1)] = \deg(x^2 + x + 1) = 2$$

$$|\lambda(\mathbb{Q}(\alpha_1))| = |G(K/\mathbb{Q}(\alpha_1))| = |\langle(2,3)\rangle| = 2$$

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = 3 = (G(K/F) : G(K/\mathbb{Q}(\alpha_1))) = \frac{|G(K/F)|}{|G(K/\mathbb{Q}(\alpha_1))|}$$

Exam Problem 2019

a) Let K be the splitting field of x^3-2 over $\mathbb{Q}$. Find $[K:\mathbb{Q}]$ and the Galois group $G(K/\mathbb{Q})$

b) Let K be the splitting field over $\mathbb{Q}$ of $f(x) \in \mathbb{Q}[x]$ where $\deg f(x) = 3$. Let A_3 denote the alternating subgroup of S_3. Show $G(K/\mathbb{Q}) = A_3$ if and only if $K = \mathbb{Q}(\alpha)$ for α a root of $f(x)$.

c) Conclude all roots of $f(x)$ from part b) must be in $\mathbb{R}$.